Fraud Prevention Presentation
Max Reedy, Senior Analyst

Max Reedy, Senior Analyst in the Criminal Investigation (CI) Office of Refund Crimes, talked about preventing online fraud. Refund Crimes uses an "IP Strategy" to identify filers of fraudulent online returns. A description of the IP Strategy was provided along with the challenges it faces and updates that are planned for 2004.

The presentation started with an example of the type of online filing fraud where the filer cannot be identified using traditional fraud detection methods. This worse case scenario occurs when someone steals someone else's identity. They then use that stolen identity to file a fraudulent return online. They also use the stolen identity to set up a bank account. Even if one of CI's Fraud Detection Centers determines this return is false there is no way for them to find the filer without using the IP Strategy.

The IP Strategy consists of five pieces of data that is either captured when the online return is received by the IRS e-file Transmitter or determined by the Fraud Detection Center calling the Transmitter. The five pieces of data are the "IP Address", "IP Date", "IP Time", time zone and whether or not standard or daylight savings time is used. The owner of the IP Address, normally an Internet Service Provider, is notified to preserve the pertinent connection log by the Fraud Detection Center. A Special Agent serves a summons on the IP Address owner in order to get the connection log and other information. The connection log shows which account holder was using the IP address in question at the requested time.

The IP Strategy is facing the following challenges. If any of the 5 pieces of data are missing the filer cannot be identified. If the IP address is a reserved the filer cannot be identified. As far as Internet technology, if the Transmitter does not capture the IP address of the filer's ISP's "firewall" then identifying the filer might be impossible. As far as business practices, if the IP address owner turns out to be someone who does not keep connection logs then the filer cannot be identified.

In demonstrating the impact of these challenges on the IP Strategy the 2003 online filing figures through April were used to show the following. Approximately 9% of all online returns had invalid IP addresses. Another 9% had reserved IP addresses. About 1% was both invalid and reserved. An unknown percentage has either missing IP data, an IP address that belonged to the Transmitter or the IP address owner did not keep connection logs.

The two types of IP addresses in use, IPv4 and IPv6, were described. Invalid IP addresses were defined. The current IP Address field will be enlarged in 2004 to

allow the capture of IPv6 addresses. A link to a web site that details reserved IPv4 addresses was provided.

A new Summary Record field will be created for 2004, the "IP Time Zone". This two-character field will consist of the time zone and a standard or daylight savings indicator, for example, "ES" is Eastern Standard time. The use of Coordinated Universal Time (UTC), also known as GMT or Zulu was briefly discussed. Additional information about UTC can be found at "greenwichmeantime.com".

All online returns with missing IP data or invalid IP addresses will be rejected for 2004. Online returns with reserved IPv4 addresses will result in the Transmitter being sent an acknowledgement. The Transmitter should determine why a reserved IPv4 address was captured and what can be done in the future to prevent it.

Three other new Summary Record fields are being requested for 2004, "IP Routing Transit Number", "IP Depositor Account Number", and "IP Email Address". The IP Email Address will be used to detect refunds that are going to the same address. Currently, only the address on the return is used to do this. The filer's bank account information is needed because when a RAL is obtained only the RAL account appears on the return. Having the filer's bank account information will allow detection of returns where multiple refunds are being deposited into the same bank account. The ETA Policy Board will make a decision about whether or not these three fields will be added in July.

After answering a fielding three questions (two about how a RAL results in the IRS not knowing the filer's true bank account and another about the amount of online fraud), the presentation was closed with a solicitation for suggestions to improve the IP Strategy. Max can be reached at 202-927-4063 or emailed at max.reedy@ci.irs.gov.